

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073337

(43)Date of publication of application : 18.03.1997

(51)Int. Cl. G06F 1/00

G06F 9/06

G06F 17/60

H04N 7/16

(21)Application number : 07-227843 (71)Applicant : CANON INC

(22)Date of filing : 05.09.1995 (72)Inventor : IWAMURA KEIICHI

(54) CHARGING DEVICE, INFORMATION RECEPTION DEVICE, AND COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To adequately charge information use of a user of a multimedia network, etc., while easily performing management and protecting the privacy of the user.

SOLUTION: When the user inputs money information to a PPC input part 14 provided for a user terminal 10 by using cash, a prepaid card, an IC card, etc., a decision part 11 decides whether or not provided information PP can be used according to the amount of money that the money information shows and/or the provided information PP from an information provider P and a signal processing part 17 processes and outputs the provided information PP to the user in response to a signal allowing the user.

LEGAL STATUS

[Date of request for examination] 21.12.1998

[Date of sending the examiner's decision of rejection] 27.06.2000

[Kind of final disposal of
application other than the
examiner's decision of rejection or
application converted registration]
[Date of final disposal for
application]
[Patent number]
[Date of registration]
[Number of appeal against 2000-011557
examiner's decision of rejection]
[Date of requesting appeal against 27.07.2000
examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Accounting equipment equipped with a judgment means to output the enabling signal with which use of the provided information which judges the money information inputted from an input means by which the money information which shows the amount of money recorded on the record medium is inputted, and the above-mentioned input means, and is offered by the information provider is permitted.

[Claim 2] The above-mentioned judgment means is accounting equipment according to claim 1 which was made to judge based on the above-mentioned money information and the use tariff information added to the above-mentioned provided information.

[Claim 3] Accounting equipment according to claim 1 whose above-mentioned money information is cash.

[Claim 4] The above-mentioned record medium is accounting equipment according to claim 1 which is an IC card.

[Claim 5] The information receiving set equipped with an input means by which the money information which is the information receiving set accomplished so that the provided information offered by the information provider might be received, and shows the amount of money is inputted, and a judgment means to output the enabling signal with which the money information inputted from the above-mentioned input means is judged, and use of the above-mentioned provided information is permitted.

[Claim 6] The above-mentioned judgment means is the information receiving set according to claim 5 which was made to judge based on the above-mentioned money information and the use tariff information added to the above-mentioned provided information.

[Claim 7] The information receiving set according to claim 5 whose above-mentioned money information is cash.

[Claim 8] The above-mentioned money information is an information receiving set according to claim 5 which is the information recorded on the record medium.

[Claim 9] The information receiving set [equipped with the means of communications which transmits the use information on the above-mentioned provided information outside] according to claim 5.

[Claim 10] Communication system which accomplished and was equipped with the accounting equipment which has a judgment means to output the enabling signal with which the inputted money information is judged and use of the above-mentioned provided information is permitted so that money information might be inputted as the information provider terminal unit which offers information, and the user-terminal equipment which receives and uses the provided information from the above-mentioned information provider terminal unit.

[Claim 11] The above-mentioned judgment means is the communication system according to claim 10 which was made to judge based on the above-mentioned money information and the use tariff information added to the above-mentioned provided information.

[Claim 12] Communication system according to claim 10 whose above-mentioned money information is cash.

[Claim 13] The above-mentioned money information is communication system according to claim 10 which is the information recorded on the record medium.

[Claim 14] Communication system according to claim 10 which prepared the means of communications which transmits the use information on provided information to the above-mentioned user-terminal equipment.

[Claim 15] Communication system according to claim 14 which formed the tariff portioner terminal unit which transmits tariff distribution information to the above-mentioned information provider terminal unit according to the above-mentioned use information.

[Claim 16] Communication system according to claim 14 which formed the tariff payment terminal unit which processes by the use tariff of provided information paying for another according to the above-mentioned use information.

[Claim 17] Claim 10 which was made to perform the communication link

between each above-mentioned equipment by cryptocommunication, communication system of 14-16 given in any 1 term.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the charging system especially to informational offer and informational it about the accounting equipment, the information receiving set, and communication system which are used in the multimedia network which transmits information, such as dynamic-image data, static-image data, voice data, computer data, and a computer program.

[0002]

[Description of the Prior Art] In recent years, with maintenance of the optical fiber network in a trunk communication network, the spread of cable television systems, utilization of satellite communication, the spread of Local Area Networks, etc., various information is offered using this communication network, and the so-called information service industry which collects a tariff according to the contents and the amount of the information is increasing. In such service, it becomes important to perform accounting to the offered information appropriately.

[0003] However, if actual, protection of information is imperfect and unjust use of a program or image (voice is included) information has been a problem. In order to prevent this unjust use, an anti-copying function is attached, or the software equipment item number which is equivalent to the software itself at the above-mentioned equipment item number is given using the hardware equipment item number given to the computer etc., and there is the technique of collating two equipment item numbers at the time of program execution. However, the anti-copying function was inconvenient at the times, such as backup, and equipment item number collating was inconvenient about equipment item number management or sale, and was not so practical.

[0004] On the other hand, the concept which aimed at protection of the right of the software rightful claimant (henceforth, information provider) a "superdistribution" was proposed by Mr. Ryoichi Mori, and was shown in each official report, such as JP, 60-77218, A, JP, 60-191322, A, JP, 64-68835, A, JP, 02-44447, A, and JP, 04-64129, A. Drawing 10 is the

conceptual diagram of the "superdistribution" shown in JP, 04-64129, A. An information provider P sends the software P_{Pi} (or P_{Pj}) which he created to a user terminal 10. A user terminal 10 judges the use propriety of Software PP in the judgment section 11 according to the conditions for every user ID of the proper data P_{IDI} (or P_{IDj}) to which it was added by Software PP, and a user, if use is good, the use hysteresis of provided information will be recorded on the storage section 12, and an information provider P will charge the use tariff of the provided information (software PP) etc. based on the hysteresis. 13 is SSU (software service unit) containing the above each part.

[0005]

[Problem(s) to be Solved by the Invention] However, the "superdistribution" method mentioned above had the following troubles. (1) "superdistribution" needs to establish the storing means of user proper data at least, in order to judge whether you are the user permitted to the information provider with user proper data, such as user ID, therefore to realize a "superdistribution." By such method, a user needs to apply for informational use to an information provider beforehand, needs to get his user ID etc., and needs to register as 1 user proper data. It is complicated to manage the user proper data with which the procedure of such a use application differs from many like user ID.

[0006] (2) In order that "superdistribution" may prevent informational unjust use, or in order that an information provider may grasp the use situation of his provided information, it has a use software hysteresis storing means like the storage section 12, and an information provider performs the claim of a tariff etc. to a user based on the hysteresis. Although this use hysteresis is needed in order that information may carry out not acquisition but rental-treatment in a "superdistribution", by such method, it will be known by the information provider what kind of information the user used, and a user's privacy cannot be protected.

[0007] (3) "superdistribution" grasps the use condition of provided information correctly, namely, although it is a method for grasping a use tariff correctly, the means or method of a tariff which are related for paying are not contained. For this reason, after an information provider gets to know the use condition of provided information, other means need to perform a claim and collection of a tariff.

[0008] This invention is made in view of the above actual condition, and it aims at offering the charging system which can solve the problem of above-mentioned (1) - (3).

[0009]

[Means for Solving the Problem] In the accounting equipment by invention of claim 1, the money information inputted from an input means by which the money information which shows the amount of money is inputted, and the above-mentioned input means was judged, and a judgment means to output the enabling signal with which use of the provided information offered by the information provider is permitted is established.

[0010] An input means to by which the money information which is the information receiving set accomplished so that the provided information offered by the information provider might be received in the information receiving set by invention of claim 5, and shows the amount of money is inputted, and a judgment means output the enabling signal with which the money information inputted from the above-mentioned input means is judged, and use of the above-mentioned provided information is permitted have established.

[0011] It accomplished and the accounting equipment which has a judgment means output the enabling signal with which the inputted money information is judged and use of the above-mentioned provided information is permitted provides so that money information may input as the information provider terminal unit which offers information, and the user-terminal equipment which receive and use the provided information from the above-mentioned information offer terminal unit in the communication system by invention of claim 10.

[0012]

[Function] Since according to this invention a judgment means judges the use propriety of a user's provided information based on the money information recorded on record media, such as cash or a prepaid card, and an enabling signal is outputted when use is good, a user can get provided information in operating a user terminal etc. using this enabling signal.

[0013]

[Embodiment of the Invention] Hereafter, the gestalt of the 1st operation concerning this invention is explained with reference to drawing 1. In drawing 1 the user terminal as an information receiving set and P 10 An information provider, The provided information provided for counter value with P_{Pi} (or P_{Pj}) by the information provider P, The information proper data of a proper with which P_{IDi} (or P_{IDj}) was added to P_{Pi}, The money information recorded on cash, a card, etc. as PPC mentions later, the accounting section in which the input section of PPC and 15 contain a display in, and, as for 16, 14 contains each part 14 and 15 of the above and the judgment section 11, the judgment section 11 judges the use propriety of provided information PP to be, and 17 are

the signal-processing sections.

[0014] Next, actuation is explained. An information provider P offers the provided information PP including PID. In case the provided information PP is used, the user terminal 10 is constituted so that it may surely go via the accounting section 16. This accounting section 16 has the input section 14 as a receiving window of PPC which is money information. If the use demand of provided information PP arises, the judgment section 11 will check the availability of provided information PP based on PID and/or PPC. less than the balance that the money information on PPC shows [the use tariff shown in PID] ***** -- etc. -- it is a check. It processes and, as for the signal-processing section 17, use outputs so that O.K. (authorization) or no (NG) is notified to the signal-processing section 17, and it may become possible for a user to use [of provided information PP] it, if it is O.K. The information (the use tariff of provided information, balance of PPC, etc.) about PID and PPC at this time is displayed by the display 15. Moreover, the judgment result of the use propriety of the judgment section 11 can also be displayed by the display 15.

[0015] The money information PPC in this invention may be actual money (cash), may be a prepaid card like a telephone card, and may be electronic information equivalent to the money stored in a floppy disk and an IC card, PCMCIA, etc. In this invention, the use propriety of provided information PP is judged using the money information PPC independent of a user, not using [instead] user ID as user proper data for every user. Therefore, since a user only pays the tariff to the information which there is no need of carrying out application procedure for getting user ID, and is used as it has the money information PPC equivalent to actual money, he is natural and easy. It becomes unnecessary to manage much user proper information, and the problem of the above (1) is solved by this.

[0016] Moreover, since it does not have user proper data, as for a user, he is not known for this invention by the information provider in the privacy which information to have used. Although this seems not to protect an information provider's P right, it is not necessary to know to the privacy of the user which user corner for it to have been enough for the information provider P if only the tariff according to the use frequency of its provided information was paid, and to have used the information on. Although it does not have a use hysteresis storing means which information PID the user with which user ID used, in this invention, it can have a notice means of use to tell using the use frequency storing means or the present provided information which

information was used how many times. In drawing 1 , use frequency information is told to an information provider P according to the path shown by the dotted line. In addition, a concrete use frequency storing means or the notice means of use is explained in full detail with the gestalt of the 2-6th operations mentioned later. The problem of ply PASHI of the user of the above (2) is also solved by the above.

[0017] In this invention, since PPC is information equivalent to money, it is equivalent to payment of a tariff to use PPC itself. The problem of the above (3) is also solved by this. in addition, the concrete method of PPC coming to hand and the concrete collecting method, and the method of distributing a tariff should be involved with the problem of the above (2) -- it is shown in the gestalt of operation of **** 2-6.

[0018] In addition, although the accounting section 16 is accounting equipment of this invention and this is prepared in the interior of a user terminal 10 in one by drawing 1 , the accounting section 16 may be formed in another object in a user terminal 10. In that case, it is good as a configuration to which reception and signal processing of provided information PP are permitted from an information provider P to the use terminal unit 10 based on the signal which the accounting section 16 receives first the information PID added to provided information PP, and shows that the judgment result of the judgment section 11 based on PID and PPC is O.K. Moreover, such a configuration may be applied to the gestalt of the 2nd - the 8th operation mentioned later.

[0019] Next, the gestalt of the 2nd operation is explained about drawing 2 . Drawing 2 shows the case where PPC is actual money (cash). The input section 14 of PPC in this case is the inlet port of coin or a bill, and a user puts fixed money into this input section 14 first. When the money exceeds the tariff shown in PID, the judgment section 11 permits use of provided information PP. Or the accounting section 16 displays the use tariff of provided information on a user by the display 15, and a user inputs the money equivalent to it into the input section 14 of PPC. The judgment section 11 judges the use propriety of provided information PP based on it. Moreover, when a tariff is updated according to time amount, that is displayed and you may make it input the surcharge according to it. Moreover, the inputted amount of money is stored in the coin box 18, and a certain engine which performs recovery of an information provider P or a tariff collects it. At this time, the use frequency for every provided information PP is recorded and collected by the counter 19, and the tariff of the coin box 18 is distributed to each information provider P according to that use frequency. A counter 19 can be omitted when the number of provided information PP is one, and use frequency is

unnecessary.

[0020] Next, the gestalt of the 3rd operation is explained about drawing 3 . Drawing 3 shows the case where PPC is a prepaid card like a telephone card. A user puts a prepaid card in the input section 14 of PPC, and from the use tariff (this amount of money may be displayed) the amount of money indicated by it was indicated to be to PID, the judgment section 11 judges many, and when many, he permits use of PP. In this case, even if the use tariff of PP is updated by time amount, the input 14 of the judgment section 11 and PPC is constituted so that it may become available continuously, if it is in the tariff of a prepaid card. When it considers as the configuration whose input section 14 can add and insert a prepaid card, use of the further long duration also becomes possible.

[0021] Acquisition of such a prepaid card is easily [anywhere] available, if it is the selling gestalt marketed by many dealers like a current telephone card. In this case, the manufacturing company of a prepaid card becomes the tariff portioner 20, and an information provider P receives distribution of the tariff according to the use frequency of provided information PP by registering with that tariff portioner 20. The above-mentioned dealer is included in a charge portioner.

[0022] Distribution of the tariff according to this use frequency are realized when the accounting section 16 tells the tariff portioner 20 about current use information using communication link I/F21. This notice of use is constituted so that it may be restricted and outputted at the time at which the accounting section 16 updates the amount of money of a prepaid card. When inputting provided information PP by communication link, this communication link I/F21 can be shared. In this case, as shown in drawing 4 , the tariff portioner's 20 terminal, an information provider's P terminal, and the user terminal 10 are connected to the network 22, and the tariff portioner 20 distributes a tariff to an information provider P according to the above-mentioned notice.

[0023] Moreover, when it does not have communication link I/F21, there is also a method of changing the class of prepaid card according to the information to be used. At this time, the judgment section 11 performs processing in which the class of prepaid card is investigated according to information, and also judges the use propriety to it. Moreover, when a means to record use record of provided information PP on a prepaid card is formed in the accounting section 16 and the tariff portioner 20 collects these prepaid cards, the tariff according to use frequency can

also be distributed. In that case, what is necessary is in exchange of a prepaid card, to end with the tariff of only money information, and just to make it into the selling gestalt of the tariff of the prepaid card itself also being added besides the tariff of money information, when it is not exchange of a prepaid card in order to promote recovery of a prepaid card. However, the tariff corresponding to unrecoverable use record may be distributed by the ratio according to the use record currently collected.

[0024] Drawing 5 shows the gestalt of the 4th operation and shows the case where PPC is a floppy disk or an electric and/or magnetic device with easy rewriting. Moreover, a network system is shown in drawing 6. In this case, the money information stored in PPC is special data which can carry out addition processing only by the tariff portioner 20 who is data guaranteed by a bank, other financial institutions, etc., or includes a dealer. A user puts PPC in the input section 14. The accounting section 16 reads information from PPC, and when the accounting section 16 can ask PPC for a use tariff, the judgment section 11 permits more (this amount of money may be displayed) use of PP than the tariff that amount of money was indicated to be to PID (O.K.). In this case, continuously, even if the use tariff of PP is updated by time amount, less than the written tariff of PPC is constituted so that it may be available.

[0025] Since the money information in this case is electronic information, the communication link in a predetermined procedure with the tariff portioner 20 can also perform I/O of money information through communication link I/F21. Since a user does not necessarily pay actual money to the tariff portioner 20 directly at this time unlike the gestalt of the 1st and the 2nd operation, the bank and the other financial institutions (henceforth, tariff payment person 23) which contracted the contract with the user guarantee the money payment of a user. Furthermore, distribution of the tariff according to use frequency are attained also about the notice of use information by telling the tariff portioner 20 about the present use information using communication link I/F21 like the gestalt of the 3rd operation. In this case, it is also possible to remit a use tariff to the direct tariff portioner 20 or an information provider P using the electronic money information PPC.

[0026] Specifically, I/O of electronic money information is realizable with the following communications processing. Moreover, the accounting section 16 shall have the code and an authentication processing means like the after-mentioned, and shall have a means to manage safely the

time stamp shown by TA mentioned later. Since PPC is a medium with easy rewriting of a floppy disk etc. and injustice may be performed by the copy of PPC etc., in order to prevent it, authentication of PPC of this is enabled, and it opposes injustice, such as a copy of PPC, by management of a time stamp.

[0027] Next, a user is set to A, C and a tariff payment person are set [an information provider] to D for B and a tariff portioner, each holds secretly the private key which can sign, and a communications partner explains accounting as what knows the public key which can inspect the signature (for example, the private key of A is set to s_A and a public key is set to p_A). Here, the case where A uses the provided information P_i of B is considered. However, a processing result with the key Y of X shall be expressed with $\{X\}^Y$, and each processing of a user and management of a key or a type stamp shall be based on storage and record of the means or everybody to whom the safety in the accounting section 16 was guaranteed.

[0028] [Money information acquisition processing]

(1) A gives its registration information $i_A(s)$ (the account number, credit number, etc.), signs with a private key s_A , and sends the input request of the money information worth a yen (the unit of currency is not restricted to a circle) to C.

$MA = \{A, \{A, i_A, a, TA\}^{s_A}\}$

[0029] (2) If the signature of MA is inspected with the public key p_A of A, D is asked for a cyclotomy using i_A and it is accepted, C will sign every yen and every base unit c (if information is the price of a 100 yen unit, it is every 100 yen) in the money information a by s_C which is the signature key of C, and will send the following message to A.

However, a different time stamp TC_i is attached to them.

$MC = \sigma \{TA, \{C, e, TC_i\}^{s_C}\}^{p_A}$ [0030] (3) A decodes each of MC by p_A , inspects a signature with the public key p_C of C corresponding to s_C further, and if an inspection result is right, it will record $\{C, a, TC_i\}^{s_C}$ on PPC. In addition, TA and TC_i show a time stamp and the message with the same time stamp from the same transmitting person is taken as an unjust demand. Moreover, if [are / like / or TA and TC_i do not have being a serial number or that it is in agreement by chance / a small random number], they may not be a time stamp.

[0031] [Notice processing of use information]

(1) When A wants to use Information P_i , if larger than the use tariff the money information in PPC of A was indicated to be to PID_i , the accounting section 16 will permit use of P_i .

(2) When A ends use of P_i , the accounting section 16 eliminates during

use the use tariff required from the money information on PPC.

[0032] (3) At this time, A sends the next notice MB of use to C. However, the eliminated use tariff is set to b.

$MB = \{A, B, \{B, b, TB\}^s A\}$

(4) C inspects this message and pays b yen as a dividend to B at the time of the right.

[0033] In the above-mentioned explanation, in order to simplify processing, the cipher system between C and each user was made into public key encryption, but if the key is shared beforehand, it is clear that a common key cryptosystem may be used. Moreover, the shelf-life of each message can also be set by the time amount from a time stamp. The order of a list in a message may be above in random order, and a user's identifier or time stamp which are shown by A, B, etc. may not necessarily be required for it. Furthermore, the procedure of the above-mentioned money information acquisition processing and the notice processing of use information is one example, and all the things that perform accounting, without using user proper data by making electronic information into money information are contained in this invention.

[0034] Moreover, when it does not have communication link I/F21, a user has the money information of the tariff portioners 20, such as a dealer, stored in PPC by the way inputted in exchange for a tariff. Moreover, in case [of the tariff portioners 20, such as a dealer,] money information is filled up and inputted by the way, when the accounting section 16 records use record of said provided information PP like MB on PPC, and a supplement machine collects use records for PPC, the tariff according to use frequency can be distributed. Since such electronic money information is special data which only the tariff portioner 20 can process as mentioned above, in order for the user without communication link I/F21 to use PPC, use records can surely be collected through the tariff portioners 20, such as a dealer, and distribution of the tariff according to use frequency are possible.

[0035] Drawing 7 shows the gestalt of the 5th operation and shows the case where PPC is an IC card and an electronic card like PCMCIA. The configuration of a network system is the same as that of drawing 6. In this case, the money information stored in PPC is special data which can carry out addition processing only by the tariff portioner 20 who is data guaranteed by a bank, other financial institutions, etc., or includes a dealer. A user puts PPC in the input section 14 of PPC, and enables actuation of PPC in predetermined procedure (inspection of a personal identification number etc.). The accounting section 16 reads money information from PPC, and when the accounting section 16 can ask

PPC for a use tariff, the judgment section 11 permits more (the amount of money may be displayed) use of PP than the tariff the frame was indicated to be to PID. In this case, continuously, even if the use tariff of PP is updated by time amount, less than the written tariff of PPC is constituted so that it may be available.

[0036] Since the money information in this case is electronic information, the communication link in a predetermined procedure with the tariff portioner 20 can also perform I/O of money information through communication link I/F21. Since a user does not necessarily pay actual money to the tariff portioner 20 directly at this time unlike the gestalt of the 1st and the 2nd operation, the bank and the other financial institutions 23 which contracted the contract with the user, i.e., a tariff payment person, guarantee the money payment of a user. Furthermore, distribution of the tariff according to use frequency are attained also about the notice of use information by telling the tariff portioner 20 about the present use information using communication link I/F21 like the gestalt of the 3rd operation. In this case, it is also possible to remit a use tariff to the direct tariff portioner 20 or an information provider P using electronic money information.

[0037] Specifically, I/O of electronic money information is realizable with the following communications processing. However, the electronic card used as PPC in consideration of the safety about a communication link or processing shall perform the owner check by the personal identification number, the access control to the data memory by the access condition, and the code and authentication by cipher system like the after-mentioned as a security function. At this time, the private key used for cipher processing or authentication processing shall be written in the memory area by which the access control was carried out as mentioned above, and only those who fulfill that access condition shall access (a card publisher, tariff portioner, etc.). Moreover, it shall be the specification which cannot change the following accounting actuation except publisher [of a card], or tariff portioner 20, either.

[0038] The user terminal 10, an information provider's P terminal, the tariff portioner's 20 terminal, and the tariff payment person's 23 terminal are connected like drawing 6 in the network 22. Set a user to A and C and a tariff payment person are set [an information provider] to D for B and a tariff portioner here. C shall share the private key for cryptocommunication to each user (for example, the private key between sA, B, and C is set to sB for the private key between A and C), C shall hold secretly the private key sC for the signature which he knows, and the check key pC of the signature corresponding to it shall be exhibited.

The case where A uses the provided information P_i of B for below is considered. However, a cipher with the key Y of Plaintext X shall be expressed with $\{X\}^Y$, and the whole of each processing of a user shall be performed within PPC with the above security functions.

[0039] [Money information acquisition processing]

(1) A gives its registration information $iA(s)$ (the account number, credit number, etc.) to C, and sends the input request of the money information worth a yen (the unit of currency is not restricted to a circle) to it at C. [to D]

$MA = \{A, \{A, iA, a, TA\}^{sA}\}$

[0040] (2) If it decodes by sA which is sharing a part for the cryptopart of MA with A, D is asked for a cyclotomy using iA and it is accepted, C will sign the money information a by sC which is the signature key of C, and will send the following message to A.

$MC = \{TA, \{C, a, TC\}^{sC}\}^{sA}$ [0041] (3) A decodes MC by sA , inspect a signature with the public key pC of C corresponding to sC further, and, as for PPC of A, only in a right case, an inspection result adds the money information on a cyclotomy. Above TA and TC is time stumps and the message with the same time stump from the same transmitting person considers it as an unjust demand. Moreover, if [are / like / or TA and TC do not have being a serial number or that it is in agreement by chance / a small random number], they may not be a time stump.

[0042] [Notice processing of use information]

(1) When A wants to use Information P_i , if larger than the use tariff the money information in PPC of A was indicated to be to PID_i , the accounting section 16 will permit use of P_i .

(2) When A ends use of P_i , during use, the accounting section 16 deducts the use tariff required from the money information on PPC, and writes in the result at PPC.

[0043] (3) At this time, A sends the next notice of use to C. However, the deducted use tariff is set to b .

$MB = \{A, \{B, b, TB\}^{sA}\}$

(4) C decodes this message and pays b yen as a dividend to B at the time of the right.

[0044] Next, what is necessary is just to perform the next processing between the above-mentioned money information acquisition processing and the notice processing of use information, when also exchanging the information between A and B by cryptocommunication. However, C presupposes that the private key is shared also with an information provider.

[0045] [Information use processing]

(1) A sends the following message to C, in order to request generation of a conversation key with B from C.

$MA' = \{A, B, TA'\}$

(2) C generates the conversation key CK and sends the following message to A.

TC' , and $\{A, CK\}^sB, TA'$, and $MC' = \{B, CK\}^sA$ [0046 —] (3) A decodes MC' by sA and sends TC' , and $\{A, CK\}^sB$ to B.

(4) B sends to A the information which decoded the received message by sB and was enciphered with the conversation key CK.

(5) A decodes encryption information with the conversation key CK.

[0047] Although the cipher system between C and each user was made into the common key cryptosystem in the above-mentioned explanation in order to simplify processing, it is clear that public key encryption may be used like the gestalt of the 5th operation. Moreover, the shelf-life of each message can also be set by the time amount from a time stamp. Moreover, the order of a list in a message may be in random order, and a user's identifier or time stamp which are shown by A, B, etc. may not necessarily be required. Furthermore, the procedure of the above-mentioned money information acquisition processing and the notice processing of use information is one example, and all the things that perform accounting, without using user proper data by making electronic information into money information are contained in this invention.

[0048] Moreover, when it does not have communication link I/F21, a user has the money information of the tariff portioners 20, such as a dealer, stored in PPC by the way inputted. Moreover, in case [of the tariff portioners 20, such as a dealer,] money information is filled up and inputted by the way, when the accounting section 16 records use record of provided information PP on PPC, and a supplement machine collects use records for this PPC, the tariff according to use frequency can be distributed. Since such electronic money information is special data which only the tariff portioner 20 can process as mentioned above, in order for the user without communication link I/F21 to use PPC, use records can surely be collected through the tariff portioners 20, such as a dealer, and distribution of the tariff according to use frequency are possible.

[0049] Drawing 8 does not show the gestalt of the 6th operation and shows the charging system which the tariff portioner 20 does not need like the gestalt of the 5th operation, using electronic information as money information. The user terminal 10, an information provider's P terminal, and the tariff payment person's 23 terminal are connected like drawing 9 in the network 22. Furthermore, the electronic card used as

PPC shall perform the owner check by the personal identification number, the access control to the data memory by the access condition, and the code and authentication by the cipher system as a security function. At this time, the secret key used for cipher processing or authentication processing presupposes that it is written in the memory area by which the access control was carried out as mentioned above. Moreover, suppose that it is also the following accounting actuation the specification which cannot be changed except the publisher of a card.

[0050] The user should be set to A, B and a tariff payment person should be set to D for the information provider, each should hold secretly the private key which can sign, and the communications partner shall know the public key which can inspect the signature (for example, the private key of A is set to s_A and a public key is set to p_A). Here, the case where A uses the provided information P_i of B is considered. However, a processing result with the key Y of X shall be expressed with $\{X\}^Y$, and the whole of each processing of a user shall be performed within PPC with the above security functions.

[0051] [Money information acquisition processing]

(1) A gives its registration information $i_A(s)$ (the account number, credit number, etc.), signs with a private key s_A , and sends the input request of the money information worth a yen (the unit of currency is not restricted to a circle) to D.

$MA = \{A, \{A, i_A, a, TA\}^{s_A}\}$

[0052] (2) D inspects the signature of MA with A and a public key p_A , i_A is right, and if a yen payment [A] is possible, it will sign the money information a by D, and will send the following message to A.

$MD = \{TA, \{D, a, TD\}^{s_D}\}^{s_A}$ [0053] (3) A inspects MD by p_A , inspect a signature with the public key p_D of D corresponding to s_D further, and, as for PPC of A, only in a right case, an inspection result adds the money information on a cyclotomy. The above, TA, and TD are time stumps and the message with the same time stump from the same transmitting person is taken as an unjust demand. Moreover, TA and TD may not have being a serial number or that it is in agreement by chance, or you may not be a time stump if [like a small random number].

[0054] [Notice processing of use information]

(1) When A wants to use Information P_i , if larger than the use tariff the money information in PPC of A was indicated to be to PID_i , an accounting means will permit use of P_i .

(2) When A ends use of P_i , during use, the accounting section 16 deducts the use tariff required from the money information on PPC, and writes in the result at PPC.

[0055] (3) At this time, A sends the next notice MB of use to B. However, the deducted use tariff is set to b.

$MB = \{A, B, \{B, b, TB\}^sA\}$

(4) B inspects a signature, at the time of the right, shows signature $\{B, b, TB\}^sA$ of A to D, and receives the tariff of b.

[0056] Next, when also exchanging the information between A and B by cryptocommunication, a direct partner's public key can also perform cryptocommunication by the public key, but when there is much amount of information, cryptocommunication by the common key cryptosystem can also be performed as follows. In this case, suppose that the common key cryptosystem means is shared between each user and an information provider. However, in following (1) and (2), A and B may be reverse.

[0057] [Information use processing]

(1) A enciphers and sends the common key CK with B with the public key pB of B.

$MA' = \{A, B, CK, TA'\}^{pB}$ (2) B decodes a received message by sB .

(3) B sends the information common-key-encryptosystem-ized with the common key CK to A.

(4) A decodes common key encryptosystem-ized information with the common key CK.

[0058] Although the cipher system of D, each user, and an information provider P was made into public key encryption in the above-mentioned explanation in order to simplify explanation, it is clear that the above common key encryptosystems may be used. Moreover, the shelf-life of each message can also be set by the time amount from a time stump. Moreover, the order of a list in a message may be in random order, and a user's identifier or time stump which are shown by A, B, etc. may not necessarily be required. Furthermore, the procedure of the above-mentioned money information acquisition processing and the notice processing of use information is one example, and all the things that perform accounting, without using user proper data by making electronic information into money information are contained in this invention.

[0059] Next, the gestalt of other operations is explained.

With the charging system using the actual money shown in the gestalt of operation of the gestalt 2nd of the 7th operation, an information provider P or the tariff portioner 20 runs the facility in which one or more user terminals 10 were installed, and when many people pay money like a public telephone, a game center, a teahouse, and a library, the accounting system of using a user terminal 10 freely can be realized.

[0060] Moreover, with the charging system using the prepaid card shown in the gestalt of the 3rd operation, an information provider P

distributes provided information PP widely by CD-ROM, personal computer communications, etc., it becomes the tariff portioner 20 an engine [like a copyright association] as opposed to [whose] information is, a prepaid card is manufactured and sold, and a user purchases a prepaid card through a dealer etc. and can realize the accounting system of using provided information PP at a house, other terminals, etc.

[0061] with the charging system using the floppy disk show in the gestalt of the 4th operation , do not need the special input section 14 for PPC in the gestalt of the 3rd operation (the input section 14 of a floppy disk usually presuppose at a user terminal that it attach) , but make a dealer omissible by the exchange by communication link of money information , and a realizable accounting system consist of current networks easily by performing a code and authentication processing in software further .

[0062] The accounting system which made insurance more the accounting system using the gestalt of implementation of the above 4th with the charging system using electronic cards, such as an IC card shown in the gestalt of the 5th operation and PCMCIA, is realizable. The accounting system to which the tariff portioner 20 is not needed, i.e., a user and an information provider P do a direct deal through the tariff payment person 23 with the charging system shown in the gestalt of the 6th operation is realizable. Moreover, it is clear for the existing special data which are expected that this charging system and an accounting system will be put in practical use in the future to be applied also to the electronic cash treated like money. Furthermore, the above-mentioned charging system and the various accounting systems which combined the accounting system are also contained in this invention.

[0063] The gestalt current of the 8th operation and an information provider encipher much information with a different key, and dedicate to CD-ROM etc., the CD-ROM as a medium itself is cheaply sold through a dealer, and when an information provider informs a user of the cryptographic key of assignment information according to the request from a user, the charging system which charges the use countervalue of the information is known. However, by this method, the profits to the dealer which sells CD-ROM having sold provided information, even if the selling profits as a medium were obtained have the problem referred to as not being obtained.

[0064] Then, the above-mentioned problem is solvable by using the charging system by PPC shown by this invention not to use of rental-information but to informational acquisition. That is, when PPC, such as a prepaid card, also purchases a user to the CD-ROM purchase and

coincidence in a dealer, and a cryptographic key is got to know to them by the communication links (telephone etc.) with an information provider and he specifies payment by the prepaid card as them, an information provider collects use tariffs from the dealer which sold the prepaid card. Since it goes via a dealer also to the flow of an informational use tariff by this, the profits to information use can also obtain a dealer. In that case, the accounting section 16 inspects the money information on PPC, and if informational use is possible, only when decoding the encryption to information, it constitutes it so that a tariff may be subtracted from PPC. Furthermore, this PPC presupposes that it can convert into money, when not using it. At this time, PPC is manufactured for every information provider and sold like CD-ROM through a dealer. Therefore, the tariff portioner 20 does not need with the gestalt of this operation.

[0065] Moreover, in the gestalt of the 3rd operation, the notice processing of use information of a prepaid card can also make notice processing of use information insurance by things making it be the following. However, the identification number iP for every prepaid card and the private key sP corresponding to it shall be registered into the prepaid card.

[0066] [Notice processing of use information]

(1) If larger than the use tariff the money information in PPC of A was indicated to be to PIDi, CHECK will permit use of Information Pi.

(2) When A ends use of Pi, during use, CHECK deducts the use tariff required from the money information on PPC, and writes in the result at PPC.

[0067] (3) At this time, CHECK sends the next notice of use to C.

However, the use tariff to B is set to b.

$MB = \{iP, \{B, b, iP, TB\}^{\wedge} sP\}$

(4) Decode C with the private key sP which registered MB, and this message pays b yen to B as a dividend at the time of the right. The notice of use is ungenerable with this except what gets to know iP and sP.

[0068] Next, a common key encryption system and a public key cryptosystem are explained.

A [common key encryption system] common key encryption system is a cipher system (called a private key cryptosystem, a symmetry cipher system, and a conventional encryption system) which shares the same cryptographic key between a transmitting person and an addressee secretly. A common key encryption system can be divided into the stream cipher which changes the key for every block cipher enciphered with the

same key to every [of suitable length] character string (block), character string, or bit. There are a transposition cipher which replaces the sequence of an alphabetic character and is enciphered, a substitution type code which transposes an alphabetic character to other alphabetic characters in a block cipher. In this case, the conversion table of transposition or substitution serves as a cryptographic key. [0069] the BIJINERU code which uses many tables for stream cipher, the Barnum code using the key of throwing away only for 1 time, etc. are known (the detail of each code -- Chapter 2 and refer to Chapter 4). [of Ikeno, the Oyama work "present age code theory" Institute of Electronics, Information and Communication Engineers, and 1986.] moreover, a code (a detail -- referring to [of Tsujii Kasahara work "code and information security" Shokodo, and 1990.] Chapter 2) called DES (Data Encryption Standard) and FELA (Fast data Encipherment Algorithm) by which the algorithm is exhibited also in the block cipher is widely used as a commercial code.

[0070] However, since DES and FELA exhibit the algorithm, the decrypting method is also developed. Various deformation may be performed in order to oppose the decoding method. (For example) The below-mentioned count of a repeat Increase **** (C.) [H. Mayer and] S.M. Matyas: "CRYPTOGRAPHY- A New Dimension in Computer Data Security", Wiley-Interscience, Appendix D, pp.679-712, 1982 reference, Deformation of changing a key frequently (referring to Yamamoto, Iwamura, Matsumoto, and Imai: "a square mold pseudo-random number generation machine and the practical cipher system using a block cipher", Shingaku Giho, ISEC 93-29, pp.65-75, and 1993.) is proposed.

[0071] A [public-key-cryptosystem] public key cryptosystem is a cipher system which a cryptographic key differs from a decode key and holds public presentation and a decode key for a cryptographic key secretly. (a) describes public key encryption below and the description and (b) describe RSA cryptograph, respectively as a protocol and a method concrete [in (c)] at the example of representation, and (d).

[0072] (a) Since the description (1) cryptographic key and decode key of public key encryption differ from each other and a cryptographic key can be exhibited, it is not necessary to deliver a cryptographic key secretly, and key delivery is easy.

(2) Since each user's cryptographic key is exhibited, the user should memorize only each one of decode keys in secret.

(3) An authentication function for an addressee to check that the transmitting person of the sent correspondence not being imitation and its correspondence are not altered is realizable.

[0073] (b) If encryption actuation using the open cryptographic key K_p is set to $E(k_p, M)$ and decode actuation using the secret decode key k_s is set to $D(k_s, M)$ to the protocol correspondence M of public key encryption, a public-key-encryption algorithm will fulfill the following two conditions first.

[0074] (1) When k_p is given, count of $E(k_p, M)$ is easy. When k_s is given, count of $D(k_s, M)$ is easy.

(2) If k_s is not known, it will be the computational procedure of k_p and E . Even if it knows $C=E(k_p, M)$, it is difficult to determine M in respect of computational complexity.

Next, in addition to the above (1) and (2), secret communication is realizable when the following conditions of (3) are satisfied.

[0075] (3) To all the correspondence (plaintext) M , $E(k_p, M)$ can be defined and $D(k_s, E(k_p, M)) = M$ is materialized. That is, although everyone can calculate $E(k_p, M)$ since k_p is exhibited, $D(k_s, E(k_p, M))$ can be calculated and only he with a private key k_s can get M . On the other hand, in addition to the above (1) and (2), when the following conditions of (4) are satisfied, an authentication communication link is realizable.

[0076] (4) To all the correspondence (plaintext) M , $D(k_s, M)$ can be defined and $E(k_p, D(k_s, M)) = M$ is materialized. That is, only he with a private key k_s can calculate $D(k_s, M)$, and even if other men turn into him who calculates $D(k_s', M)$ using fake private key k_s' , and has k_s and clear up, since it is $E(k_p, D(k_s', M)) \neq M$, an addressee can check that the received information is unjust. Moreover, even if $D(k_s, M)$ is altered, it is set to $E(k_p, D(k_s, M)') \neq M$, and an addressee can check that the received information is unjust.

[0077] In public key encryption, the processing E which uses a public key is enciphered and the processing D using a private key is called decode. Therefore, although a transmitting person enciphers and an addressee decodes after that in secret communication, in an authentication communication link, a transmitting person will decode and an addressee will encipher after that.

[0078] A protocol in case public key encryption performs secret communication, authentication communication link, and secret communication with a signature to below from the transmitting person A to Addressee B is shown. The private key of A is set to k_{sA} , a public key is set to k_{pA} , the private key of B is set to k_{sB} and a public key is set to k_{pB} .

[0079] [Secret communication] When carrying out secret communication of the correspondence (plaintext) M from A to B, the following procedure

performs.

Step1: A enciphers M with the public key kp_B of B, and sends Cipher C to B.

$C = E(kp_B, M)$

Step2: B decodes C with its own private key ks_B , and obtains the plaintext M of a basis.

$H = D(ks_B, C)$

Since Addressee's B public key is opened to many and unspecified persons, the secret communication not only of A but all the men can be carried out to B.

[0080] [Authentication communication link] When carrying out the authentication communication link of the correspondence (plaintext) M from A to B, the following procedure performs.

Step1: A generates the transmitting sentence S with its own private key ks_A , and sends it to B.

$S = D(ks_A, M)$

This transmitting sentence S is called signature sentence, and actuation of obtaining a signature sentence is called signature. Step2: B carries out restoration conversion of the S with the public key kp_A of A, and obtains the plaintext M of a basis.

$M = E(kp_A, S)$

Supposing M checks that it is a meaningful sentence, it will attest that surely M has been sent from A. Since the transmitting person's A public key is opened to many and unspecified persons, not only B but all men can attest the signature sentence of A. Such authentication is also called digital signature.

[0081] [Secret communication with a signature] When carrying out secret communication with a signature of the correspondence (plaintext) M from A to B, the following procedure performs.

Step1: A signs M with its own private key ks_A , and makes the signature sentence S.

$S = D(kp_A, M)$

Furthermore, A enciphers S with the public key kp_B of B, and sends Cipher C to B.

$C = E(kp_B, S)$

Step2: B decodes C with its own private key ks_B , and obtains the signature sentence S.

$S = D(ks_B, C)$

Furthermore, B carries out restoration conversion of the S with the public key kp_A of A, and obtains the plaintext M of a basis.

$M = E(kp_A, S)$

Supposing M checks that it is a meaningful sentence, it will attest that surely M has been sent from A.

[0082] In addition, the sequence of giving the function in each Step of secret communication with a signature may be reversed, respectively.

That is, by the above-mentioned procedure, it is Step1: $C = E(k_B, D(k_A, M))$.

Step2: $M = E(k_A, D(k_B, C))$

Although it has become, secret communication with a signature is realizable with the following procedures.

Step1: $C = D(k_A, E(k_B, M))$

Step2: $M = D(k_B, E(k_A, C))$

(c) A typical public key cryptosystem [0083] Next, the example of a typical public key cryptosystem is given to below. As a method which can perform secret communication and an authentication communication link - RSA cryptograph (R.) [L. Rivest,] [A. Shamir] and I. Adleman: "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM, 1978, - R code (M. Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR -212, Technical Report MIT.1979), - W code (H.) [C. Williams: "A] modification of the RSA public-key encryption procedure" and IEEE Trans Inf. Theory and IT-26. -- 6 and 1980 -- - MI code (Matsumoto --) Imai: "the new algorithm of a public-key-encryption system", Shingaku Giho, IT 82-84, 1982: T. Matsumoto and H. Imai: "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symp, on Information Theory, 1983, [0084] As a method only whose secret communication is possible - MH code (R.) [C. Merkle and] M. E. Hellman: "Hiding information and signatures in knapsacks", IEEE 5 Trans, Inf. Theory, IT-24, 1978, - GS code (A.) [Shamir and] R. E. Zippel: "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans 3 Inf. Theory, IT-26, 1980, - CR code (B.) [Chor and R. L. Rivest: "A knapsack type public key cryptosystem based - arithmetic in] finite field", Proc Crypto 84, - M code (R.) [J. McEliece: "A] public-key cryptosystem based on algebraic coding theory" DSN Progress Rep, Jet Propulsion Lab 1978, - E code (T.) [E. Fiat: "A] public key cryptosystem and a signature scheme based on discrete logarithm", Proc Crypto 84 1984, - T code (on the other hand, the public key encryption using Shigeo Tsujii and "matrix decomposition is formula", Shingaku Giho, and IT 8512 and 1985), [0085] As a method which can perform only an authentication communication link - S code (A.) [Shamir: "A fast] signature scheme", Report MIT/LCS/TM -107, MIT laboratory for computer science Cambridge, Mass, 1978, - L code () [K. Schumacher: "Uniform] complexity and digital signature" Lecture Notes

in Computer Science 115 Automata Language and Programming, Eighth Colloquium Acre, Israel, 1981, - A GMY code (S. Goldwasser, S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983), - GMR code (S.) [Goldwasser,] [S. Micali] and R. L. Rivest: "A paradoxical solution to the signature problem", ACM Symp. on Foundation of Computer Science, 1984, - OSS code (H.) [Ong,] [C. P. Schnorr] and A. Shamir: "An efficient Computing, 1984, and -OS code signature (Okamoto --) scheme based on quadratic equation" and ACM Symp. on Theory of Shiroishi: "the digital signature method by the polynomial operation", IEICE TRANSACTIONS (D), J86-D, 5, and 1985: T. Okamoto and A. Shiraishi: "A fast signature scheme based on quadratic inequalities" IEEE Symp. on Theory of Computing, 1984

Various methods including **** are proposed.

[0086]

[Effect of the Invention] As explained above, according to this invention, the charging system and accounting system which solved the conventional problem shown in (1) - (3) in a multimedia network etc. mentioned above are realizable. By this, while a user uses various information cheaply in rental, protection of privacy can be performed, and an information provider can receive distribution of a use tariff according to the use frequency of provided information, without managing information use for every user. Moreover, by introducing a tariff portioner and tariff payment person including a dealer, it can include to payment of a tariff and a user-friendly accounting system can be constituted.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the gestalt of operation of the 1st of this invention.

[Drawing 2] It is the block diagram showing the gestalt of operation of the 2nd of this invention.

[Drawing 3] It is the block diagram showing the gestalt of operation of the 3rd of this invention.

[Drawing 4] It is the block diagram of the network by the gestalt of the 3rd operation.

[Drawing 5] It is the block diagram showing the gestalt of operation of

the 4th of this invention.

[Drawing 6] It is the block diagram of the network by the gestalt of the 4th and the 5th operation.

[Drawing 7] It is the block diagram showing the gestalt of operation of the 5th of this invention.

[Drawing 8] It is the block diagram showing the gestalt of operation of the 6th of this invention.

[Drawing 9] It is the block diagram of the network by the gestalt of the 6th operation.

[Drawing 10] It is a block diagram for explaining the conventional superdistribution method.

[Description of Notations]

P Information provider

PPC Money information

10 User Terminal

11 Judgment Section

14 PPC Input Section

16 Accounting Section

17 Signal-Processing Section

20 Tariff Portioner

21 Communication Link I/F

22 Network

23 Tariff Payment Person

【特許請求の範囲】

【請求項1】 記録媒体に記録された金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定し、情報提供者から提供される提供情報の利用を許可する許可信号を出力する判定手段とを備えた課金装置。

【請求項2】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項1記載の課金装置。

【請求項3】 上記金銭情報が現金である請求項1記載の課金装置。

【請求項4】 上記記録媒体はICカードである請求項1記載の課金装置。

【請求項5】 情報提供者から提供される提供情報を受信するように成された情報受信装置であって、金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段とを備えた情報受信装置。

【請求項6】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項5記載の情報受信装置。

【請求項7】 上記金銭情報が現金である請求項5記載の情報受信装置。

【請求項8】 上記金銭情報は記録媒体に記録された情報である請求項5記載の情報受信装置。

【請求項9】 上記提供情報の利用情報を外部に送信する通信手段を備えた請求項5記載の情報受信装置。

【請求項10】 情報を提供する情報提供者端末装置と、上記情報提供者端末装置からの提供情報を受信して利用する利用者端末装置と、金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段を有する課金装置とを備えた通信システム。

【請求項11】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項10記載の通信システム。

【請求項12】 上記金銭情報が現金である請求項10記載の通信システム。

【請求項13】 上記金銭情報は記録媒体に記録された情報である請求項10記載の通信システム。

【請求項14】 上記利用者端末装置に提供情報の利用情報を送信する通信手段を設けた請求項10記載の通信システム。

【請求項15】 上記利用情報に応じて上記情報提供者端末装置に料金分配情報を送信する料金分配者端末装置を設けた請求項14記載の通信システム。

【請求項16】 上記利用情報に応じて提供情報の利用

料金の立替え処理を行う料金立替端末装置を設けた請求項14記載の通信システム。

【請求項17】 上記各装置間の通信を暗号通信により行うようにした請求項10、14～16の何れか1項記載の通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の情報を伝送するマルチメディアネットワーク等で用いられる課金装置、情報受信装置及び通信システムに関し、特に情報の提供とそれに対する課金方式に関するものである。

【0002】

【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛星通信の実用化、ローカルエリアネットワークの普及等に伴い、かかる通信網を利用して様々な情報を提供し、その情報の内容及び量に応じて料金を徴収する、いわゆる情報サービス産業が増大している。このようなサービスにおいては、提供した情報に対する課金を適切に行うことが重要となる。

【0003】しかしながら、現実では情報の保護は不完全であり、プログラムや映像（音声を含む）情報の不正利用が問題になっている。この不正利用を防ぐために、コピー防止機能を付けたり、コンピュータ等に付与されているハードウェア機番を用い、ソフトウェア自体に上記機番に相当するソフトウェア機番を付与し、プログラム実行時に、2つの機番を照合する等の手法がある。しかし、コピー防止機能はバックアップ等の際不便であるし、機番照合は機番管理や販売に関して不便であり、あまり実用的ではなかった。

【0004】これに対して、「超流通」というソフトウェア権利者（以後、情報提供者）の権利の保護をめざした概念が森亮一氏によって提案され、特開昭60-77218号、特開昭60-191322号、特開昭64-68835号、特開平02-44447号、特開平04-64129号等の各公報に示された。図10は特開平04-64129号公報に示された「超流通」の概念図である。情報提供者Pは自分が作成したソフトウェアP_i（またはP_j）を利用者端末10に送る。利用者端末10はソフトウェアPPの利用可否を、ソフトウェアPPに付加された固有データP_{Idi}（またはP_{IDj}）と利用者のユーザID毎の条件によって判定部11で判定し、利用可ならば提供情報の利用履歴を記憶部12に記録し、その履歴に基づいて情報提供者Pはその提供情報（ソフトウェアPP）の利用料金等を請求する。13は以上の各部を含むSSU（ソフトウェアサービスユニット）である。

【0005】

【発明が解決しようとする課題】しかしながら上述した「超流通」方式は次のような問題点があった。

(1) 「超流通」は情報提供者に許可された利用者であるかどうかをユーザID等の利用者固有データによって判定し、そのために「超流通」を実現するには、少なくとも利用者固有データの格納手段を設ける必要がある。このような方式では、利用者は予め情報提供者に情報の利用を申し込み、自分のユーザID等をもらい、一利用者固有データとして登録する必要がある。このような利用申し込みの手続きや、ユーザIDのような多くの異なる利用者固有データを管理することは煩雑である。

【0006】(2) 「超流通」は情報の不正利用を防止するため、または情報提供者が自分の提供情報の利用状況を把握するために、記憶部12のような利用ソフトウェア履歴格納手段を備え、その履歴に基づいて情報提供者が利用者に料金の請求等を行う。「超流通」において情報は買い取りではなくレンタル的な扱いをするために、この利用履歴は必要になるが、このような方式では、利用者がどのような情報を利用したかということが情報提供者に知られてしまい、利用者のプライバシーを保護することができない。

【0007】(3) 「超流通」は提供情報の利用状態を正しく把握する、すなわち、利用料金を正しく把握するための方式ではあるが、料金の支払いに関する手段や方式は含まれていない。このため情報提供者が提供情報の利用状態を知った後は、他の手段によって料金の請求及び徴収を行う必要がある。

【0008】本発明は上述のような実情に鑑みてなされたものであり、前述の(1)～(3)の問題を解決することのできる課金方式を提供することを目的とする。

【0009】

【課題を解決するための手段】請求項1の発明による課金装置においては、金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定し、情報提供者から提供される提供情報の利用を許可する許可信号を出力する判定手段とを設けている。

【0010】請求項5の発明による情報受信装置においては、情報提供者から提供される提供情報を受信するように成された情報受信装置であって、金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段とを設けている。

【0011】請求項10の発明による通信システムにおいては、情報を提供する情報提供者端末装置と、上記情報提供端末装置からの提供情報を受信して利用する利用者端末装置と、金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段を有する課金装置とを設けている。

【0012】

【作用】本発明によれば、現金あるいはプリペイドカード等の記録媒体に記録された金銭情報に基づいて判定手段は利用者の提供情報の利用可否を判定し、利用可のとき許可信号を出力するので、この許可信号を用いて利用者は利用者端末等を動作させることで提供情報を得ることができる。

【0013】

【発明の実施の形態】以下、本発明に係る第1の実施の形態を図1を参照して説明する。図1において、10は情報受信装置としての利用者端末、Pは情報提供者、P Pi (またはP P j) は情報提供者Pによって有償で提供される提供情報、P I D i (またはP I D j) はP P i に付加された固有の情報固有データ、P P Cは後述するように現金やカード等に記録された金銭情報、14はP P Cの入力部、15は表示部、16は上記各部14、15及び判定部11を含む課金部、11は提供情報P Pの利用可否を判定する判定部、17は信号処理部である。

【0014】次に動作について説明する。情報提供者PはP I Dを含めた提供情報P Pを提供する。利用者端末10は、その提供情報P Pを利用する際には、必ず課金部16を経由するように構成してある。この課金部16は金銭情報であるP P Cの受け口としての入力部14がある。提供情報P Pの利用要求が生じると、判定部11はP I D及び/またはP P Cに基づいて、提供情報P Pの利用可能性をチェックする。例えば、P I Dに示された利用料金がP P Cの金銭情報が示す残高以内か否かなどのチェックである。利用がOK(許可)か否(NG)かは信号処理部17に通知され、もしOKであれば、信号処理部17は利用者が提供情報P Pの利用が可能となるように処理して出力する。このときのP I DやP P Cに関する情報(提供情報の利用料金やP P Cの残高など)は表示部15で表示される。また、判定部11の利用可否の判定結果も表示部15で表示することができる。

【0015】本発明における金銭情報P P Cは実際の金銭(現金)であってもよいし、テレホンカードのようなプリペイドカードであってもよいし、フロッピーディスク及びICカードやP C M C I Aなどに格納された金銭と等価な電子的な情報であっても良い。本発明では、利用者毎の利用者固有データとしてのユーザIDを用いず、その代わりに利用者に依存しない金銭情報P P Cによって提供情報P Pの利用可否を判定する。従って、利用者はユーザIDをもらうための申し込み手続きをする必要が無く、実際の金銭と等価な金銭情報P P Cをもつだけ、即ち利用する情報に対する料金を支払うだけであるので、自然であり容易である。これによって、多くの利用者固有情報を管理する必要もなくなり前記(1)の問題が解決される。

【0016】また、本発明では利用者固有データを持た

ないため、利用者は自分がどの情報を利用したかというプライバシーを情報提供者に知られることはない。これは情報提供者Pの権利が守られていないように見えるが、自分の提供情報の利用頻度に応じた料金が支払われさえすれば情報提供者Pには十分であって、どの利用者かどの情報を利用したかという利用者のプライバシーまで知る必要はない。本発明では、どのユーザIDをもつ利用者がどの情報PIDを利用したかという利用履歴格納手段はもたないが、どの情報が何度利用されたかという利用頻度格納手段または現在提供情報を利用していることを知らせる利用通知手段を有することはできる。図1においては、点線で示す経路によって情報提供者Pに利用頻度情報が知られる。なお、具体的な利用頻度格納手段または利用通知手段については後述する第2～6の実施の形態で詳述する。以上により、前記(2)の利用者のプライバシーの問題も解決される。

【0017】本発明では、PPCは金銭と等価な情報であるので、PPCを用いること自体が料金の支払いに相当する。これによって前記(3)の問題も解決される。なお、具体的なPPCの入手法と回収法、及び料金の分配法は前記(2)の問題と絡めて第2～6の実施の形態に示される。

【0018】尚、課金部16は本発明の課金装置であり、これを図1では利用者端末10の内部に一体的に設けているが、課金部16を利用者端末10とは別体に設けてもよい。その場合、情報提供者Pから提供情報PPに付加された情報PIDを課金部16が先ず受信し、PID、PPCに基づく判定部11の判定結果がOKであることを示す信号に基づいて利用端末装置10に対して提供情報PPの受信や信号処理を許可するような構成としてよい。また、このような構成は、後述する第2～第8の実施の形態に適用してよい。

【0019】次に第2の実施の形態を図2について説明する。図2はPPCが実際の金銭(現金)である場合を示す。この場合のPPCの入力部14はコインや紙幣の入口であり、利用者はまずこの入力部14に一定の金銭を入れる。その金銭がPIDに示された料金を超えたときに判定部11は提供情報PPの利用を許可する。または、課金部16は表示部15により利用者に提供情報の利用料金を表示し、利用者はそれに相当する金銭をPPCの入力部14に入力する。判定部11はそれをもとに提供情報PPの利用可否を判定する。また、時間に応じて料金が更新される場合には、その旨を表示し、それに応じた追加料金を入力するようにしてもよい。また、入力された金額はコインボックス18に格納され、情報提供者Pまたは料金の回収を行う何らかの機関が回収する。このとき、各提供情報PP毎の利用頻度はカウンタ19に記録・回収され、その利用頻度に応じてコインボックス18の料金が各情報提供者Pに分配される。提供情報PPが一つである場合等、利用頻度が不要ない場合

にはカウンタ19は省略できる。

【0020】次に第3の実施の形態を図3について説明する。図3はPPCがテレホンカードのようなプリペイドカードである場合を示している。利用者はPPCの入力部14にプリペイドカードをさし込み、それに記載された金額がPIDに示された利用料金(この金額は表示されてもよい)より多いか否かを判定部11が判定し、多い場合にはPPの利用を許可する。この場合、PPの利用料金が時間によって更新されていっても、プリペイドカードの料金内であれば継続して利用可能となるように、判定部11とPPCの入力14は構成される。入力部14がプリペイドカードを追加して挿入できる構成とした場合はさらなる長時間の利用も可能となる。

【0021】このようなプリペイドカードの入手は現在のテレホンカードと同様に多くの販売店によって市販される販売形態になっていればどこでも容易に入手可能である。この場合、プリペイドカードの製造会社は料金分配者20となり、情報提供者Pはその料金分配者20に登録することによって提供情報PPの利用頻度に応じた料金の分配を受ける。前述の販売店は料分配者に含まれる。

【0022】この利用頻度に応じた料金の分配は、課金部16が通信I/F21を用いて現在の利用情報を料金分配者20に知らせることによって実現される。この利用通知は課金部16がプリペイドカードの金額を更新するときに限り出力されるように構成される。提供情報PPを通信によって入力する場合は、この通信I/F21を共有することができる。この場合、図4に示されるように料金分配者20の端末、情報提供者Pの端末及び利用者端末10はネットワーク22に接続されており、料金分配者20は上記通知に応じて料金を情報提供者Pに分配する。

【0023】また、通信I/F21を持たない場合は、利用する情報に応じてプリペイドカードの種類を変えるという方法もある。このとき、判定部11は情報に応じてプリペイドカードの種類を調べるという処理を行い、それに対する利用可否も判定する。また、課金部16に提供情報PPの利用記録をプリペイドカードに記録する手段を設け、このプリペイドカードを料金分配者20が回収することによって、利用頻度に応じた料金の分配を行うこともできる。その場合、プリペイドカードの回収を促進するために、プリペイドカードの交換の場合は、金銭情報のみの料金で済み、プリペイドカードの交換でない場合は、金銭情報の料金の他にプリペイドカード自体の料金も加算されるなどの販売形態にすればよい。ただし、回収できない利用記録に対応する料金は回収できなかった利用記録に応じた比率で分配しても良い。

【0024】図5は第4の実施の形態を示すもので、PPCがフロッピーディスクまたは書き換えが容易な電気的及び/または磁気的なデバイスである場合を示す。ま

た、ネットワークシステムを図6に示す。この場合、PPC内に格納される金銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者20によってのみ加算処理できる特殊なデータである。利用者は入力部14にPPCをさし込む。課金部16はPPCから情報を読み出し、その金額がPIDに示された料金より多く（この金額は表示されてもよい）、課金部16がPPCに利用料金を請求可能である場合に判定部11はPPの利用を許可（OK）する。この場合、PPの利用料金が時間によって更新されていても、PPCの記載料金以内は継続して利用可能であるように構成される。

【0025】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信1/F21を介して料金分配者20との所定の手続きによる通信によって行うことができる。このとき、第1、第2の実施の形態と異なり、実際の金銭を利用者は料金分配者20に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関（以後、料金立替者23）である。さらに、利用情報の通知に関しても、第3の実施の形態と同様に通信1/F21を用いて現在の利用情報を料金分配者20に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報PPCによって直接料金分配者20や情報提供者Pに送ることも可能である。

【0026】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。また、課金部16は後述のような暗号・認証処理手段を有しており、後述するTA等で示されるタイムスタンプを安全に管理する手段を有するものとする。これは、PPCがフロッピーディスク等の書き換えが容易な媒体であるために、PPCのコピー等によって不正が行われる可能性があるため、それを防止するためにPPCを認証可能にし、タイムスタンプの管理によってPPCのコピー等の不正に対抗するものである。

【0027】次に、利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの（例えば、Aの秘密鍵をsA、公開鍵をpAとする）として課金処理を説明する。ここで、AがBの提供情報Piを利用する場合を考える。ただし、Xの鍵Yによる処理結果を{X}^Yで表し、利用者の各処理及び鍵やタイムスタンプの管理は課金部16内の安全性が保証された手段または各人の記憶や記録によるものとする。

【0028】[金銭情報入手処理]

(1) Aはa円（通貨の単位は円に限らない）分の金銭情報の入力要求を自分の登録情報iA（口座番号やクレジット番号など）をつけて秘密鍵sAで署名しCに送

る。

$$MA = \{A, \{A, iA, a, TA\}^sA\}$$

【0029】(2) CはMAの署名をAの公開鍵pAで検査し、iAを用いてDにa円分の請求を行い、それが受け入れられれば金銭情報aを1円毎または基本単位c毎（情報が100円単位の価格であれば100円毎）にCの署名鍵であるsCで署名して次のメッセージをAに送る。ただし、それらには異なるタイムスタンプTCiがつけられる。

$$MC = \Sigma \{TA, \{C, e, TCi\}^sC\}^pA$$

【0030】(3) AはMCの各々をpAで復号し、さらにsCに対応するCの公開鍵pCで署名を検査し、検査結果が正しければ{C, a, TCi}^sCをPPCに記録する。なお、TA、TCiはタイムスタンプを示すものであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、TA、TCiはシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

【0031】[利用情報通知処理]

(1) Aが情報Piを利用したいとき、AのPPC内の金銭情報がPIDに示された利用料金より大きければ課金部16はPiの利用を許可する。

(2) AがPiの利用を終了したとき、または利用中に課金部16はPPCの金銭情報から要した利用料金を消去する。

【0032】(3) このとき、Aは次の利用通知MBをCに送る。ただし、消去された利用料金をbとする。

$$MB = \{A, B, \{B, b, TB\}^sA\}$$

(4) Cはこのメッセージを検査し正しいときに、b円をBへの分配金として支払う。

【0033】上記の説明では、処理を簡単にするためにCと各利用者間の暗号方式は公開鍵暗号としたが、予め鍵が共有されていれば共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、A、B等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【0034】また、通信1/F21を持たない場合、利用者は販売店などの料金分配者20のところでPPCに格納する金銭情報を料金と引き替えに入力してもらう。また、課金部16が前記MBのような提供情報PPの利用記録をPPCに記録し、PPCを販売店等の料金分配者20のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような

電子的な金銭情報は前述したように料金分配者20だけが処理できる特殊なデータであるので、通信1/F21を持たない利用者はPPCを用いるためには必ず販売店等の料金分配者20を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

【0035】図7は第5の実施の形態を示すもので、PPCがICカードやPCMCIAのような電子的なカードである場合を示す。ネットワークシステムの構成は図6と同一である。この場合は、PPC内に格納される金銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者20によってのみ加算処理できる特殊なデータである。利用者はPPCの入力部14にPPCをさし込み、所定の手続き（暗証番号の検査など）によってPPCを動作可能にする。課金部16はPPCから金銭情報を読み出し、その額がPIDに示された料金より多く（金額は表示されてもよい）、課金部16がPPCに利用料金を請求可能である場合に判定部11はPPの利用を許可する。この場合、PPの利用料金が時間によって更新されていても、PPCの記載料金以内は継続して利用可能であるように構成される。

【0036】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信1/F21を介して料金分配者20との所定の手続きによる通信により行うことができる。このとき、第1、第2の実施の形態と異なり実際の金銭を利用者は料金分配者20に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関、即ち、料金立替者23である。さらに、利用情報の通知に関しても、第3の実施の形態と同様に通信1/F21を用いて現在の利用情報を料金分配者20に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報によって直接料金分配者20や情報提供者Pに送ることも可能である。

【0037】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。ただし、通信や処理に関する安全性を考慮してPPCとして用いる電子的なカードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、後述のような暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密鍵は前述のようにアクセス制御されたメモリ領域に書き込まれ、そのアクセス条件を満たす者（カード発行者や料金分配者等）しかアクセスできないものとする。また、以下の課金動作もカードの発行者または料金分配者20以外変更できない仕様になっているものとする。

【0038】利用者端末10、情報提供者Pの端末、料金分配者20の端末、料金立替者23の端末は図6のよ

うにネットワーク22で接続されている。ここで、利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、Cは各利用者に対して暗号通信のための秘密鍵を共有し（例えば、AとCの間の秘密鍵をsA、BとCの間の秘密鍵をsBとする）、Cは自分しか知らない署名のための秘密鍵sCを秘密に保持し、それに対応する署名の検査鍵pCを公開しているものとする。以下に、AがBの提供情報Piを利用する場合を考える。ただし、平文Xの鍵Yによる暗号文を{X}^Yで表し、利用者の各処理は全て上述のようなセキュリティ機能をもつPPC内で行われるものとする。

【0039】[金銭情報入手処理]

(1) AはCにa円（通貨の単位は円に限らない）分の金銭情報の入力要求をDへの自分の登録情報iA（口座番号やクレジット番号など）をつけてCに送る。

$MA = \{A, \{A, iA, a, TA\}^sA\}$

【0040】(2) CはMAの暗号部分をAと共有しているsAで復号し、iAを用いてDにa円分の請求を行い、それが受け入れられれば金銭情報aにCの署名鍵であるsCで署名して次のメッセージをAに送る。

$MC = \{TA, \{C, a, TC\}^sC\}^sA$

【0041】(3) AはMCをsAで復号し、さらにsCに対応するCの公開鍵pCで署名を検査し、検査結果が正しい場合のみAのPPCはa円分の金銭情報を加算する。上記TAやTCはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、TA、TCはシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

【0042】[利用情報通知処理]

(1) Aが情報Piを利用したいとき、AのPPC内の金銭情報がPIDに示された利用料金より大きければ課金部16はPiの利用を許可する。

(2) AがPiの利用を終了したとき、または利用中に課金部16はPPCの金銭情報から要した利用料金を差し引き、その結果をPPCに書き込む。

【0043】(3) このとき、Aは次の利用通知をCに送る。ただし、差し引いた利用料金をbとする。

$MB = \{A, \{B, b, TB\}^sA\}$

(4) Cはこのメッセージを復号し正しいときに、b円をBへの分配金として支払う。

【0044】次に、AとBの間の情報も暗号通信によってやりとりする場合、次の処理を前述の金銭情報入手処理と利用情報通知処理の間で行えばよい。ただし、Cは情報提供者とも秘密鍵を共有しているとする。

【0045】[情報利用処理]

(1) AはCにBとの会話鍵の生成を依頼するために次のメッセージをCに送る。

$MA' = \{A, B, TA'\}$

(2) Cは会話鍵CKを生成し、次のメッセージをAに

送る。

$MC' = \{ \{TC', A, CK\} \wedge sB, TA', B, CK\} \wedge sA$

【0046】(3) Aは MC' を sA で復号し、 $\{TC', A, CK\} \wedge sB$ をBに送る。

(4) Bは受信メッセージを sB で復号し、会話鍵 CK で暗号化した情報をAに送る。

(5) Aは会話鍵 CK で暗号化情報を復号する。

【0047】上記の説明では、処理を簡単にするためにCと各利用者間の暗号方式は共通鍵暗号としたが、第5の実施の形態と同様に公開鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、A、B等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【0048】また、通信1/F21を持たない場合、利用者は販売店などの料金分配者20のところでPPCに格納する金銭情報を入力してもらう。また、課金部16が提供情報PPの利用記録をPPCに記録し、このPPCを販売店等の料金分配者20のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような電子的な金銭情報は前述したように料金分配者20だけが処理できる特殊なデータであるので、通信1/F21を持たない利用者はPPCを用いるためには必ず販売店等の料金分配者20を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

【0049】図8は第6の実施の形態を示すもので、第5の実施の形態と同様に電子的な情報を金銭情報として用い、料金分配者20のいらない課金方式を示すものである。利用者端末10、情報提供者Pの端末、料金立替者23の端末は図9のようにネットワーク22で接続されている。さらに、PPCとして用いる電子カードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密の鍵は前述のようにアクセス制御されたメモリ領域に書き込まれているとする。また、以下の課金動作もカードの発行者以外変更できない仕様になっているとする。

【0050】利用者をA、情報提供者をB、料金立替者をDとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの（例えば、Aの秘密鍵を sA 、公開鍵を pA とする）とする。ここで、AがBの提供情報Piを利用する場合を

考える。ただし、Xの鍵Yによる処理結果を $\{X\} \wedge Y$ で表し、利用者の各処理は全て上述のようなセキュリティ機能をもつPPC内で行われるものとする。

【0051】[金銭情報入手処理]

(1) Aは a 円（通貨の単位は円に限らない）分の金銭情報の入力要求を自分の登録情報iA（口座番号やクレジット番号など）をつけて秘密鍵 sA で署名しDに送る。

$MA = \{A, \{A, iA, a, TA\} \wedge sA\}$

【0052】(2) DはMAの署名をAと公開鍵 pA で検査し、iAが正しくAが a 円支払可能であれば、金銭情報 a をDで署名して次のメッセージをAに送る。

$MD = \{TA, \{D, a, TD\} \wedge sD\} \wedge sA$

【0053】(3) AはMDを pA で検査し、さらに sD に対応するDの公開鍵 pD で署名を検査し、検査結果が正しい場合のみAのPPCは a 円分の金銭情報を加算する。上記、TAやTDはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、TA、TDはシリアル番号や偶然一致することがない、または少ない乱数のようなものであれば、タイムスタンプでなくてもよい。

【0054】[利用情報通知処理]

(1) Aが情報Piを利用したいとき、AのPPC内の金銭情報がPiDiに示された利用料金より大きければ課金手段はPiの利用を許可する。

(2) AがPiの利用を終了したとき、または利用中に課金部16はPPCの金銭情報から要した利用料金を差し引き、その結果をPPCに書き込む。

【0055】(3) このとき、Aは次の利用通知MBをBに送る。ただし、差し引いた利用料金を b とする。

$MB = \{A, B, \{B, b, TB\} \wedge sA\}$

(4) Bは署名を検査し正しいときに、Aの署名 $\{B, b, TB\} \wedge sA$ をDに示し、 b の料金を受け取る。

【0056】次に、AとBの間の情報も暗号通信によってやりとりする場合、直接相手の公開鍵で公開鍵による暗号通信を行うこともできるが、情報量が多い場合次のように共通鍵暗号による暗号通信を行うこともできる。この場合、各利用者と情報提供者の間には共通鍵暗号手段が共有されているとする。ただし、下記の(1)、

(2)においてAとBは逆であっても良い。

【0057】[情報利用処理]

(1) AはBとの共通鍵CKをBの公開鍵 pB で暗号化して送る。

$MA' = \{A, B, CK, TA'\} \wedge pB$

(2) Bは受信メッセージを sB で復号する。

(3) Bは共通鍵CKで共通鍵暗号化した情報をAに送る。

(4) Aは共通鍵CKで共通鍵暗号化情報を復号する。

【0058】上記の説明では、説明を簡単にするためにDと各利用者と情報提供者Pとの暗号方式は公開鍵暗号

としたが、前述のような共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、A、B等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【0059】次に、その他の実施の形態を説明する。

第7の実施の形態

第2の実施の形態に示す実際の金銭を用いた課金方式によって、1つ以上の利用者端末10を設置した施設を情報提供者Pまたは料金分配者20が営業し、公衆電話やゲームセンター、喫茶店、図書館のように多くの人が金銭を支払うことによって自由に利用者端末10を使用するという課金システムが実現できる。

【0060】また、第3の実施の形態に示すプリペイドカードを用いた課金方式によって、情報提供者PがCD-ROMやパソコン通信等によって広く提供情報Pを配布し、情報に対する著作権協会のような機関が料金分配者20となってプリペイドカードを製作・販売し、利用者は販売店などを通じてプリペイドカードを購入し、自宅やその他の端末等で提供情報Pを利用するという課金システムが実現できる。

【0061】第4の実施の形態に示すフロッピーディスクを用いた課金方式によって、第3の実施の形態におけるPPCのための特殊な入力部14を必要とせず（利用者端末には通常フロッピーディスクの入力部14はついているとする）、さらに金銭情報の通信によるやりとりによって販売店を省略可能とし、暗号・認証処理をソフト的に行うことによって現在のネットワークで容易に実現可能な課金システムが構成できる。

【0062】第5の実施の形態に示すICカードやPCMCIA等の電子的なカードを用いた課金方式によって、上記第4の実施の形態を用いた課金システムをより安全にした課金システムが実現できる。第6の実施の形態に示す課金方式によって、料金分配者20のいらない、即ち利用者と情報提供者Pとが料金立替者23を通して直接取引をする課金システムが実現できる。また、この課金方式及び課金システムは将来実用化されると思われるある特殊なデータを金銭と同様に扱う電子現金に対しても適用可能であることは明らかである。さらに、上記の課金方式、及び課金システムを組み合わせた種々の課金システムも本発明に含まれる。

【0063】第8の実施の形態

現在、情報提供者が多くの情報を異なる鍵で暗号化してCD-ROM等に納め、媒体としてのCD-ROM自体は販売店を通じて安価に販売し、利用者からの依頼に応じて情報提供者が利用者に指定情報の暗号鍵を知らせる

ときにその情報の利用対価を請求する課金方式が知られている。しかし、この方式ではCD-ROMを販売する販売店は媒体としての販売利益は得られても、提供情報を販売したことに対する利益は得られないと言う問題がある。

【0064】そこで、本発明で示したPPCによる課金方式をレンタル的な情報の利用ではなく、情報の買い取りに対して用いることによって上記の問題が解決できる。即ち、利用者は販売店でのCD-ROM購入と同時に、プリペイドカード等のPPCも購入し、情報提供者との通信（電話など）によって暗号鍵を知るときにプリペイドカードでの支払を指定することによって、情報提供者はそのプリペイドカードを販売した販売店から利用料金を回収する。これによって、情報の利用料金の流れに対しても販売店を経由するので、販売店は情報利用に対する利益も得ることができる。その場合、課金部16はPPCの金銭情報を検査し、情報の利用が可能であれば、情報に対する暗号化を復号するときだけPPCから料金を引くように構成する。さらに、このPPCは使用しないときには換金できるとする。このとき、PPCは情報提供者毎に製作され、販売店を通じてCD-ROMと同様に販売される。従って、この実施の形態では料金分配者20は必要としない。

【0065】また、第3の実施の形態において利用情報通知処理を以下のようにすることで、プリペイドカードの利用情報通知処理も安全にすることができる。ただし、プリペイドカードにはプリペイドカード毎の識別番号iPとそれに対応した秘密鍵sPとが登録されているものとする。

【0066】[利用情報通知処理]

(1) AのPPC内の金銭情報がPIDiに示された利用料金より大きければCHECKは情報Piの利用を許可する。

(2) AがPiの利用を終了したとき、または利用中にCHECKはPPCの金銭情報から要した利用料金を差し引き、その結果をPPCに書き込む。

【0067】(3) このとき、CHECKは次の利用通知をCに送る。ただし、Bへの利用料金をbとする。

$MB = \{iP, \{B, b, iP, TB\}^sP\}$

(4) CはMBを登録した秘密鍵sPで復号し、このメッセージが正しいときにb円をBへ分配金として支払う。これによって、iPとsPを知るもの以外、利用通知を生成することはできない。

【0068】次に、共通鍵暗号方式及び公開鍵暗号方式について説明する。

【共通鍵暗号方式】共通鍵暗号方式は送信者と受信者で同一の暗号鍵を秘密に共有する暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）である。共通鍵暗号方式は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と文字列ま

たはビットごとに鍵を変えていくストリーム暗号に分けることができる。ブロック暗号には文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に置き換える換字式暗号等がある。この場合、転置や換字の対応表が暗号鍵となる。

【0069】ストリーム暗号には多表を用いるビジネル暗号や1回限りの使い捨ての鍵を用いるバーナム暗号等が知られている(各暗号の詳細は池野、小山著「現代暗号理論」電子情報通信学会、1986.の第2章及び第4章参照)。また、ブロック暗号のなかでもアルゴリズムが公開されているDES(Data Encryption Standard)やFELA(Fast data Encipherment ALgorithm)といった暗号(詳細は辻井、笠原著「暗号と情報セキュリティ」昭晃堂、1990.の第2章参照)が商用暗号として広く用いられている。

【0070】ただし、DESやFELAはアルゴリズムを公開しているために暗号解読法も開発され、その解読法に対抗するために種々の変形が行われていることがある(例えば、後述の繰り返し回数を増したり(C. H. Mayer and S. M. Matyas: "CRYPTOGRAPHY-A New Dimension in Computer Data Security", Wiley-Interscience, Appendix D, pp. 679-712, 1982参照)、鍵を頻繁に変える(山本、岩村、松本、今井:

"2乗型疑似乱数生成器とブロック暗号を用いた実用的暗号方式", 信学技報, ISEC93-29, pp. 65-75, 1993. 参照)などの変形が提案されている)。

【0071】【公開鍵暗号方式】公開鍵暗号方式は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。以下公開鍵暗号について(a)で特徴、(b)でプロトコル、(c)で代表例、(d)で具体的な方式としてRSA暗号についてそれぞれ述べる。

【0072】(a)公開鍵暗号の特徴

(1)暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(2)各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

(3)送られてきた通信文の送信者が偽物でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0073】(b)公開鍵暗号のプロトコル
通信文Mに対して、公開の暗号鍵Kpを用いた暗号化操作をE(kp, M)とし、秘密の復号鍵ksを用いた復号操作をD(ks, M)とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

【0074】(1)kpが与えられたとき、E(kp, M)の計算は容易である。ksが与えられたとき、D(ks, M)の計算は容易である。

(2)もし、ksを知らないなら、kpとEの計算手順とC=E(kp, M)を知っていても、Mを決定することは計算量の点で困難である。

次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

【0075】(3)全ての通信文(平文)Mに対し、E(kp, M)が定義でき、D(ks, E(kp, M))=Mが成立する。つまり、kpは公開されているため誰もがE(kp, M)を計算することができるが、D(ks, E(kp, M))を計算してMを得ることができるのは秘密鍵ksを持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

【0076】(4)すべての通信文(平文)Mに対し、D(ks, M)が定義でき、E(kp, D(ks, M))=Mが成立する。つまり、D(ks, M)を計算できるのは秘密鍵ksを持っている本人のみであり、他の人が偽の秘密鍵ks'を用いてD(ks', M)を計算し、ksを持っている本人になりましたとしても、E(kp, D(ks', M))≠Mなので受信者は受けとった情報が不正なものであることを確認できる。また、D(ks, M)が改ざんされてもE(kp, D(ks, M)')≠Mとなり、受信者は受けとった情報が不正なものであることを確認できる。

【0077】公開鍵暗号では、公開鍵を用いる処理Eを暗号化、秘密鍵を用いる処理Dを復号と呼んでいる。従って、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【0078】以下に公開鍵暗号により送信者Aから受信者Bへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。Aの秘密鍵をksA、公開鍵をkpAとし、Bの秘密鍵をksB、公開鍵をkpBとする。

【0079】【秘密通信】AからBへの通信文(平文)Mを秘密通信する場合次の手順で行う。

Step 1: AはBの公開鍵kpBでMを暗号化し、暗号文CをBに送る。

C=E(kpB, M)

Step 2: Bは自分の秘密鍵ksBでCを復号し、もとの平文Mを得る。

H=D(ksB, C)

受信者Bの公開鍵は不特定多数に公開されているので、Aに限らず全ての人がBに秘密通信できる。

【0080】【認証通信】AからBへの通信文(平文)Mを認証通信する場合次の手順で行う。

Step 1: Aは自分の秘密鍵ksAで送信文Sを生成

しBに送る。

$S = D(k_s A, M)$

この送信文Sを署名文といい、署名文を得る操作を署名という。Step 2: BはAの公開鍵 $k_p A$ でSを復元変換し、もとの平文Mを得る。

$M = E(k_p A, S)$

もしMが意味のある文であることを確認したならば、Mが確かにAから送られてきたことを認証する。送信者Aの公開鍵は不特定多数に公開されているので、Bに限らず全ての人がAの署名文を認証できる。このような認証をデジタル署名ともいう。

【0081】[署名付秘密通信] AからBへの通信文

(平文) Mを署名付秘密通信する場合次の手順で行う。

Step 1: Aは自分の秘密鍵 $k_s A$ でMを署名し、署名文Sを作る。

$S = D(k_p A, M)$

さらにAはBの公開鍵 $k_p B$ でSを暗号化し、暗号文CをBに送る。

$C = E(k_p B, S)$

Step 2: Bは自分の秘密鍵 $k_s B$ でCを復号し、署名文Sを得る。

$S = D(k_s B, C)$

さらに、BはAの公開鍵 $k_p A$ でSを復元変換し、もとの平文Mを得る。

$M = E(k_p A, S)$

もし、Mが意味のある文であることを確認したならば、Mが確かにAから送られてきたことを認証する。

【0082】なお、署名付秘密通信の各Step内における関数を施す順序はそれぞれ逆転してもよい。すなわち、上記の手順では、

Step 1: $C = E(k_p B, D(k_s A, M))$

Step 2: $M = E(k_p A, D(k_s B, C))$

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step 1: $C = D(k_s A, E(k_p B, M))$

Step 2: $M = D(k_s B, E(k_p A, C))$

(c) 代表的な公開鍵暗号方式

【0083】次に代表的な公開鍵暗号方式の例を以下に挙げる。秘密通信と認証通信ができる方式として

・RSA暗号(R. L. Rivest, A. Shamir and L. Adleman: "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM, 1978)、

・R暗号(M. Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR-212, Technical Report MIT, 1979)、

・W暗号(H. C. Williams: "A modification of the RSA public-key encryption procedure", IEEE Trans. Inf. Theory, IT-26, 6, 1980)、

・MI暗号(松本、今井: "公開鍵暗号系の新しいアルゴリズム", 信学技報, IT82-84, 1982:

T. Matsumoto and H. Imai: "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symp. on Information Theory, 1983)、

【0084】秘密通信のみができる方式として

・MH暗号(R. C. Merkle and M. E. Hellman: "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24, 5, 1978)、

・GS暗号(A. Shamir and R. E. Zippel: "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans. Inf. Theory, IT-26, 3, 1980)、

・CR暗号(B. Chor and R. L. Rivest: "A knapsack type public key cryptosystem based on arithmetic in finite field", Proc. Crypto 84)、

・M暗号(R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory" DSN Progress Rep. Jet Propulsion Lab 1978)、

・E暗号(T. E. ElGamal: "A public key cryptosystem and a signature scheme based on discrete logarithm", Proc. Crypto 84, 1984)、

・T暗号(辻井重男, "行列分解を利用した公開鍵暗号の一方式", 信学技報, IT8512, 1985)、

【0085】認証通信のみができる方式として

・S暗号(A. Shamir: "A fast signature scheme", Report MIT/LCS/TM-107, MIT laboratory for computer science Cambridge, Mass, 1978)、

・L暗号 (K. Lieberherr: "Uniform complexity and digital signature" Lecture Notes in Computer Science 115 Automata Language and Programming, Eighth Colloquium Acre, Israel, 1981)、
 ・GMY暗号 (S. Goldwasser, S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983)、
 ・GMR暗号 (S. Goldwasser, S. Micali and R. L. Rivest: "A paradoxical solution to the signature problem", ACM Symp. on Foundation of Computer Science, 1984)、
 ・OSS暗号 (H. Ong, C. P. Schnorr and A. Shamir: "An efficient signature scheme based on quadratic equation", ACM Symp. on Theory of Computing, 1984)、
 ・OS暗号 (岡本、白石: "多項式演算によるデジタル署名方式", 信学論 (D), J86-D, 5, 1985; T. Okamoto and A. Shiraishi: "A fast signature scheme based on quadratic inequalities" IEEE Symp. on Theory of Computing, 1984)
 などをはじめ様々な方式が提案されている。

【0086】

【発明の効果】以上説明したように、本発明によれば、マルチメディアネットワーク等における前述した(1)～(3)に示した従来の問題を解決した課金方式及び課金システムが実現できる。これによって、利用者は種々の情報をレンタル的に安価に利用しながらプライバシーの保護ができ、情報提供者は利用者毎の情報利用の管理

を行うことなく、提供情報の利用頻度に応じて利用料金の分配を受けることができる。また、販売店を含む料金分配者や料金立替者を導入することによって、料金の支払いまで含めて使い勝手の良い課金システムを構成することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すブロック図である。

【図2】本発明の第2の実施の形態を示すブロック図である。

【図3】本発明の第3の実施の形態を示すブロック図である。

【図4】第3の実施の形態によるネットワークのブロック図である。

【図5】本発明の第4の実施の形態を示すブロック図である。

【図6】第4、第5の実施の形態によるネットワークのブロック図である。

【図7】本発明の第5の実施の形態を示すブロック図である。

【図8】本発明の第6の実施の形態を示すブロック図である。

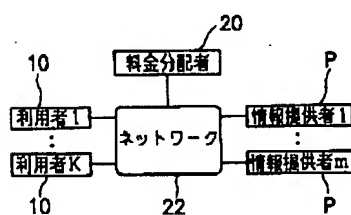
【図9】第6の実施の形態によるネットワークのブロック図である。

【図10】従来の超流通方式を説明するためのブロック図である。

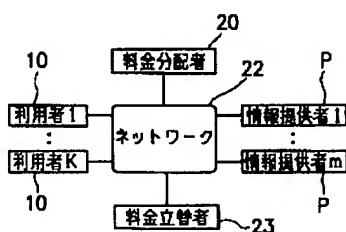
【符号の説明】

P 情報提供者
 PPC 金銭情報
 10 利用者端末
 11 判定部
 14 PPC入力部
 16 課金部
 17 信号処理部
 20 料金分配者
 21 通信I/F
 22 ネットワーク
 23 料金立替者

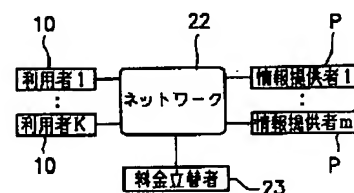
【図4】



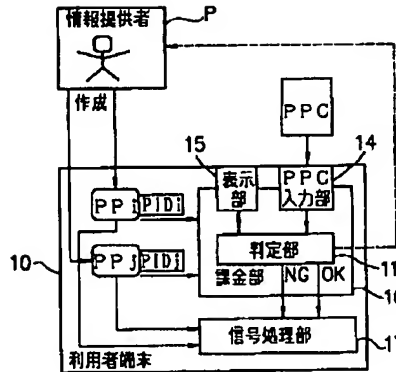
【図6】



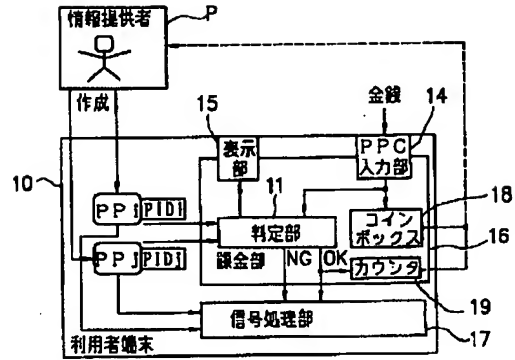
【図9】



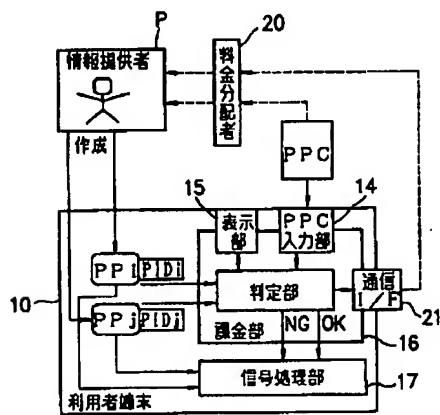
【図1】



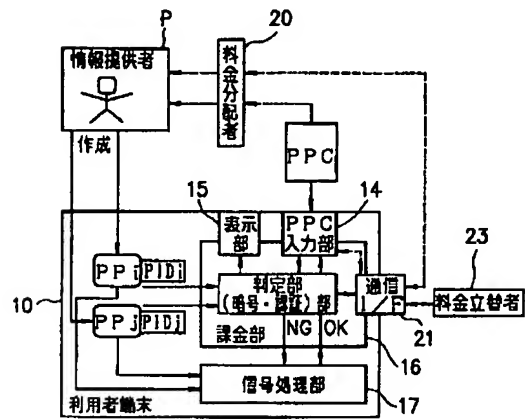
【図2】



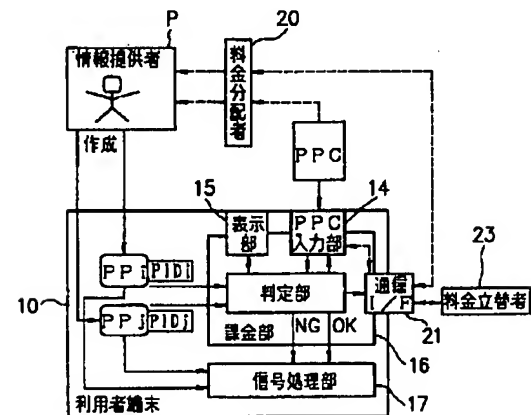
【図3】



【図5】



【図7】



【図8】

